

11/28/06

n. 207 # 5  
n. 278 # 11, 12

Chinese Remainder Thm Assume  $R$  commut.

Def Two ideals are comaximal if  $A+B=R$ .

Ex  $m\mathbb{Z}$  &  $n\mathbb{Z}$  are comaximal iff  $(m,n)=1$ .

Theorem (Chinese Remainder Thm) Let  $A_1, \dots, A_k$  be ideals in  $R$ . Then

$\exists$  a homomorphism

$$\psi: R \rightarrow R/A_1 \times R/A_2 \times \dots \times R/A_k$$

$$r \mapsto (r+A_1, r+A_2, \dots, r+A_k)$$

w/ kernel  $A_1 A_2 \dots A_k$ .

Moreover if  $i \neq j \Rightarrow A_i + A_j$  are comaximal then  $\psi$  is onto,

$$A_1 \dots A_k = A_i \dots A_k \text{ so}$$

$$R/A_1 \dots A_k \cong R/A_i \times \dots \times R/A_k$$

Proof Assume  $k=2$ . Before "moreover" is obvious

Suppose  $1=xy$   $x \in A_1, y \in A_2$ . Then  $\psi$

$$\psi(x) = (0, 1) \quad \psi(y) = (1, 0) \text{ so } \psi \text{ is onto.}$$

$$\text{Now } (r+A_1, r+A_2) = \psi(r, x+ry)$$

Finally  $A_1 A_2 \subseteq A_1 A_2$  Let  $c \in A_1 A_2$  Then

$$c = cx + cy \in A_1 A_2 \quad //$$

Example 1.  $\gcd(n, 1) = 1 \Rightarrow \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$

2. Let  $n = p_1^{a_1} \dots p_k^{a_k}$  Then  
 $\phi(n) = \phi(p_1^{a_1}) \phi(p_2^{a_2}) \dots \phi(p_k^{a_k})$   $\phi = \text{Euler } \phi$

Motivation for the pump

Suppose  $m_1, \dots, m_k \in \mathbb{Z}$  w/  $(m_i, m_j) = 1 \quad i \neq j$

Solve:  $x \equiv a_1 \pmod{m_1} \quad x \equiv a_2 \pmod{m_2} \quad \dots \quad x \equiv a_k \pmod{m_k}$

has! solution mod  $n = m_1 \dots m_k$

Proof:  $\mathbb{Z}/(m_1 \dots m_k)\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \longleftarrow \mathbb{Z}$

pull back  $(a_1, a_2, \dots, a_k)$  since onto.

Chapter 8 SPECIAL TYPES OF INTEGRAL DOMAINS

\*  $R$  is commutative \*

Def Let  $R$  be an integral domain. A norm on  $R$  is a map  $N: R \rightarrow \mathbb{Z}^{\geq 0}$  w/  $N(a) = 0 \Rightarrow a = 0$ . It is positive if  $N(a) = 0 \Rightarrow a = 0$ .

Example 1.  $\mathbb{Z} = R, N(a) = |a|$   
 2.  $\mathbb{R} = \mathbb{Z}[x], N(p(x)) = \deg p(x)$  very weak

Def. An integral domain is a Euclidean Domain if  $\exists$  norm  $N$  on  $R$  so  $\forall a, b \in R, b \neq 0, \exists q, r \in R$  with

$$a = qb + r \quad r = 0 \text{ or } N(r) < N(b)$$

$\uparrow$   $\uparrow$   
 quotient remainder

i.e.  $R$  has a division algorithm.

Remark Euclidean domains have division algorithms.

$$\begin{aligned}
 a &= q_0 b + r_0 \\
 b &= q_1 r_0 + r_1 \\
 r_0 &= q_2 r_1 + r_2 \\
 &\vdots \\
 r_{n-2} &= q_{n-1} r_{n-1} + r_n \\
 r_{n-1} &= q_n r_n
 \end{aligned}$$

must terminate

\*\* Not necessarily unique \*\*  
 \*\* May be different  $N$ 's \*\*

Examples

- 1. Any field, any norm! (remainder always 0!)
- 2.  $\mathbb{Z}$  with  $||$  norm (long division algorithm)
- 3. FCS w/ norm = degree  
 Pract "long division" of polynomials

4. Suppose:

- a.  $K$  is a field w/ a discrete valuation  $v: K^* \rightarrow \mathbb{Z}$ .
- b.  $R \subseteq K$  is valuation ring
- c.  $K$  is field of fractions of  $R$ . ( $R$  is called a discrete valuation ring)

Thm  $R$  is a Euclidean domain where  $v = N$ .

Proof If  $v|a| < v|b|$  then  $a = 0 \cdot b + a$  ✓

If  $v|b| > v|a|$  then  $a = (b^{-1} \cdot a) \cdot b + 0$

norm  $> 0$  but  $a \in R$ .

5.  $\mathbb{Z}[i]$

Nonexamples

1.  $\mathbb{Z}/n\mathbb{Z}[x]$  is not a PID

~~2. Gaussian integers  $\mathbb{Z}[i]$  is a PID with norm  $N(a+bi) = a^2 + b^2$~~

2.  $\mathbb{Z}[\sqrt{-3}]$

Def A principal ideal domain is an integral domain in which every ideal is principal. (i.e. of form  $I = (r)$ .)

Thm Euclidean domains are PID's

Proof Let  $I \neq 0$  be an ideal. Choose  $d \in I, d \neq 0$  of minimal norm.

Then  $s \in I$ . then

$$s = dq + r \quad N(r) < N(d) \quad \text{But}$$

$$s - dq \in I \Rightarrow r = 0 \Rightarrow s \in (d) \quad //$$

Examples

1.  $\mathbb{Z}$
2.  $\mathbb{F}[x]$

Nonexamples

1.  $R = \mathbb{Z}[x]$   $I = (2, x)$
2.  $R = \mathbb{Z}[\sqrt{-5}]$   $I = (3, 2 + \sqrt{-5})$

then  $3 = \alpha(a + b\sqrt{-5})$  some  $a, b$   
 $2 + \sqrt{-5} = \beta(a + b\sqrt{-5})$

Let  $N = a^2 + 5b^2$

take norms  $9 = N(\beta) (a^2 + 5b^2)$  so  $a^2 + 5b^2 = 1, 3$  or  $9$

$9 \nmid 3 \Rightarrow N(\beta) = 9$

\* If  $a^2 + 5b^2 = 9$  then  $\beta = \alpha^{-1} \cdot 3$  so  $\alpha = 3$   
 so  $a + b\sqrt{-5} = 3 \neq$

6  
Goal Which familiar properties of  $\mathbb{Z}$  carry over to various commutative rings?

GLDs  $R$  comm ring

Def Let  $a, b \in R$   $b \neq 0$ . Say  $b$  divides  $a$ ,  $b|a$ , if  $a = bx, x \in R$ .

Def. Let  $a, b \in R$ . A greatest common divisor is  $d \neq 0$  in  $R$  such that

1.  $d|a, d|b$
2. If  $e|a, e|b$  then  $e|d$ .

Example  $-6$  is a gcd of  $42$  and  $12$  in  $\mathbb{Z}$ . (so is  $6$ !)

Remarks

1. In  $\mathbb{Z}$  this is the "greatest" common divisor.

2. Suppose  $(a, b) = (d)$ . Then  $d$  is a gcd of  $a$  &  $b$ .

Proof  $a \in (d)$  so  $d|a$   
 $b \in (d)$  so  $d|b$

If  $e|a$  then  $a = ex, b = ey$  so  $(a, b) \in (e)$  so  $(d) \subseteq (e)$  so  $d = e \cdot \dots$

-Not conversely! e.g. gcd  $(2, x)$  in  $\mathbb{Z}[x]$  is  $1$  but  $(2, x) \neq (1)$ .

\* can't always write

$$\text{gcd}(a, b) = \alpha a + \beta b$$

Prop In an integral domain, gcd's are "unique" up to units.

Proof Let  $d, d' \in R$  be gcd's. Thus  $d|d', d'|d$  by assumption.

Let  $d' = dx, d = d'y$  so  $d' = d'xy$  so  $d'(1-xy) = 0$   
so  $xv = 1$  so  $x, y$  units.